

Little galoisian modules

Chandan Singh Dalawat
 Harish-Chandra Research Institute
 Chhatnag Road, Jhunsi, Allahabad 211019, India
 dalawat@gmail.com

Abstract. Let p be a prime number, let K be a p -field (a local field with finite residue field of characteristic p), let L be a finite galoisian tamely ramified extension of K , and let $G = \text{Gal}(L|K)$. Suppose that L is split over K in the sense that the short exact sequence $1 \rightarrow T \rightarrow G \rightarrow G/T \rightarrow 1$ has a section, where T is the inertia subgroup of G . We determine the structure of the $\mathbf{F}_p[G]$ -module $L^\times/L^{\times p}$ in characteristic 0 when the p -torsion subgroup ${}_pL^\times$ of L^\times has order p , and of the $\mathbf{F}_p[G]$ -modules $L^\times/L^{\times p}$ and $L^+/\wp(L^+)$ in characteristic p , where $\wp(x) = x^p - x$.

Let \tilde{K} be a maximal galoisian extension of K , let V be the maximal tamely ramified extension of K in \tilde{K} , let $\Gamma = \text{Gal}(V|K)$, and let B be the maximal abelian extension of exponent p of V in \tilde{K} . We determine the structure of the $\mathbf{F}_p[[\Gamma]]$ -module $\text{Gal}(B|V)$, and show how this leads in characteristic 0 to a simple proof of the fact that the profinite group $\text{Gal}(\tilde{K}|K)$ is generated by $[K : \mathbf{Q}_p] + 3$ elements.

1. Introduction

(1) In the first part of this Note (§2), we work with a finite field k , a finite extension l of k , and an injective morphism of groups $\theta : T \rightarrow l^\times$. Let $q = \text{Card } k$, let $\Sigma = \text{Gal}(l|k)$, and let σ be the generator $x \mapsto x^q$ ($x \in l$) of Σ . View T as a submodule of the Σ -module l^\times , and let $G = T \times_q \Sigma$ be the twisted product of Σ by T . For every $i \in \mathbf{Z}$, we have the $k[G]$ -module $l(i)$ whose underlying k -space is l and on which G acts by

$$\sigma.x = x^q, \quad t.x = \theta(t)^i x \quad (x \in l, t \in T),$$

We show that these modules are projective, and determine when two such modules are isomorphic. The main tool is a lemma of Iwasawa [5, Lemma 1, p. 449].

MSC2010 : Primary 11R23, 11S15

Keywords : Local fields, galoisian modules, tame ramification

(2) In the second and third parts (§3 and §4), we work with a local field K with finite residue field k of cardinality q and characteristic p , and a finite galoisian tamely ramified split extension L of K of residue field l and group $G = \text{Gal}(L|K)$. The inertia subgroup $T \subset G$ comes with a faithful character $\theta : T \rightarrow l^\times$ and, since L is split over K by hypothesis, G is isomorphic to $T \times_q \Sigma$, where $\Sigma = \text{Gal}(l|k)$.

Exploiting our study of the $k[G]$ -modules $l(i)$ in §2, we determine the structure of the $\mathbf{F}_p[G]$ -module $L^\times/L^{\times p}$ when K has characteristic 0 and ${}_pL^\times$ has order p in §3, and of the $\mathbf{F}_p[G]$ -modules $L^\times/L^{\times p}$ and $L^+/\wp(L^+)$, where $\wp(x) = x^p - x$ ($x \in L$), when K has characteristic p in §4. The results are a generalisation from the much simpler case $L = K(\sqrt[p-1]{K^\times})$ treated in [3].

(3) In the fourth part (§5 and §6), we consider the maximal tamely ramified extension V of K of group $\Gamma = \text{Gal}(V|K)$ and, putting everything together, determine the structure of the $\mathbf{F}_p[[\Gamma]]$ -module $V^\times/V^{\times p}$ in characteristic 0 and of the $\mathbf{F}_p[[\Gamma]]$ -modules $V^\times/V^{\times p}$ and $V^+/\wp(V^+)$ in characteristic p . As a consequence, we determine (in both cases : mixed- and equi-characteristic) the structure of the $\mathbf{F}_p[[\Gamma]]$ -module $\text{Gal}(B|V)$, where B is the maximal abelian extension of V of exponent p . This is achieved by passing to the limit over the results of §3 and §4.

Finally, in §6 we take K to be a finite extension of \mathbf{Q}_p with maximal galoisian extension \tilde{K} and show how the sturcture theorem for the $\mathbf{F}_p[[\Gamma]]$ -module $\text{Gal}(B|V)$ as proved in §5 leads to a simple proof of the fact that the profinite group $\text{Gal}(\tilde{K}|K)$ is generated by $[K : \mathbf{Q}_p] + 3$ elements.

2. Iwasawa's lemma

(4) We recall a crucial lemma from Iwasawa [5] and simplify its proof. Let p be a prime number and let $e > 0$ be an integer $\not\equiv 0 \pmod{p}$. Let $g > 0$ be a multiple of the order of $\bar{p} \in (\mathbf{Z}/e\mathbf{Z})^\times$, so that there is a unique morphism of groups $\mathbf{Z}/g\mathbf{Z} \rightarrow (\mathbf{Z}/e\mathbf{Z})^\times$ such that $1 \mapsto p$. Let n be a multiple of $\text{lcm}(p-1, e)$, and write $n = c(p-1)$ and $n = d.e$. Let $b^{(i)}$ ($i > 0$) be the sequence of positive integers $\not\equiv 0 \pmod{p}$, namely $b^{(i)} = i + \lfloor (i-1)/(p-1) \rfloor$. For every $a, b \in \mathbf{Z}$, we denote by $[a, b]$ the set of *integers* between a and b .

(5) *The map $[1, n] \times \mathbf{Z}/g\mathbf{Z} \rightarrow \mathbf{Z}/e\mathbf{Z}$ sending (i, j) to $b^{(i)}p^j \pmod{e}$ is surjective and every fibre has dg elements.*

Proof. Consider the map $[1, cp] \times \mathbf{Z}/g\mathbf{Z} \rightarrow \mathbf{Z}/e\mathbf{Z}$ sending (r, j) to $rp^j \pmod{e}$; it is the “product” of the natural map of reduction \pmod{e} on the first factor and the map $1 \mapsto p$ discussed in (4) on the second factor,

and it is clearly surjective. View the interval $[1, cp]$ as the (disjoint) union of the successive intervals $[1, de]$ and $[n+1, n+c]$ on the one hand, and as the (disjoint) union of the subsets $(b^{(i)})_{i \in [1, n]}$ and $(ip)_{i \in [1, c]}$ on the other. By the *contribution* of a subset $S \subset [1, cp]$ we mean the family $(t_x)_{x \in \mathbf{Z}/e\mathbf{Z}}$, where t_x is the number of antecedents of x in $S \times \mathbf{Z}/g\mathbf{Z}$. Clearly, the contribution of $(ip)_{i \in [1, c]}$ is the same as that of $[n+1, n+c]$, because $j \mapsto j+1$ is a permutation of $\mathbf{Z}/g\mathbf{Z}$. So the contribution of $(b^{(i)})_{i \in [1, n]}$ is the same as that of $[1, de]$, which is easy to compute : for fixed $x \in \mathbf{Z}/e\mathbf{Z}$ and $j \in \mathbf{Z}/g\mathbf{Z}$, there are exactly d elements $r \in [1, de]$ such that $rp^j \equiv x \pmod{e}$. \square

(6) *The $k[\Sigma]$ -module l .* Let k be a finite extension of \mathbf{F}_p of cardinality $q = p^a$. Let l be a finite extension of k , and put $f = [l : k]$, $g = af$. Let $\Sigma = \text{Gal}(l|k)$, and denote by σ the generator $x \mapsto x^q$ ($x \in l$) of Σ . The $k[\Sigma]$ -module l is free of rank 1, as follows from the normal basis theorem [1, V.70] : there exists an $\alpha \in l$ such that $(\sigma^i(\alpha))_{i \in \mathbf{Z}/f\mathbf{Z}}$ is a k -basis of l .

(7) *The groups T , G , and the character $\theta : T \rightarrow l^\times$.* Let T be a subgroup of l^\times , e its order (so that $q^f \equiv 1 \pmod{e}$) and $\theta : T \rightarrow l^\times$ the inclusion ; the group $\text{Hom}(T, l^\times)$ of characters of T is cyclic of order e and generated by θ . Identifying $\text{Aut}(T)$ with $(\mathbf{Z}/e\mathbf{Z})^\times$, there is a unique morphism of groups $\Sigma \rightarrow \text{Aut}(T)$ such that $\sigma \mapsto q$; endow T with this action of Σ (which is the galoisian action as a subgroup of l^\times) and let $G = T \times_q \Sigma$ be the twisted product of Σ by the Σ -module T , so that $\sigma t \sigma^{-1} = t^q$ for every $t \in T$; we sometimes write $G = T\Sigma$.

(8) Concretely, if we choose a generator τ for T , then the group G has the presentation $G = \langle \sigma, \tau \mid \sigma^f = 1, \tau^e = 1, \sigma \tau \sigma^{-1} = \tau^q \rangle$, and $\theta(\tau)$ is a primitive e -th root of 1 in l . Conversely, if we choose an element $\eta \in l^\times$ of order e , then $\theta^{-1}(\eta)$ is a generator of T . In what follows, we don't need to choose τ or η .

(9) *The $k[G]$ -modules $l(r)$.* For every $r \in \mathbf{Z}$, make G act on the k -space l by the law

$$\sigma.x = x^q, \quad t.x = \theta(t)^r x, \quad (x \in l, t \in T)$$

and denote the resulting $k[G]$ -module by $l(r)$; it is clear that $l(r)$ depends only on the image $\bar{r} \in \mathbf{Z}/e\mathbf{Z}$, and that the $k[G]$ -module $l(0)$ is deduced from the $k[\Sigma]$ -module l via the map $k[G] \rightarrow k[\Sigma]$ coming from the projection $G \rightarrow \Sigma$.

(10) *The $k[G]$ -module $\bigoplus_{i \in \mathbf{Z}/e\mathbf{Z}} l(i)$ is free of rank 1.*

Proof. Indeed, the $k[\Sigma]$ -module l is free of rank 1 (6), and if $\alpha \in l$ is a $k[\Sigma]$ -basis of l , then α is a $k[G]$ -basis of $\bigoplus_{i \in \mathbf{Z}/e\mathbf{Z}} l(i)$, where the $k[G]$ -module

$l(0)$ has been identified with l as in (9). \square

(11) The $l[G]$ -module $l(r) \otimes_{\mathbf{F}_p[G]} l[G]$ is isomorphic to $\bigoplus_{j \in \mathbf{Z}/g\mathbf{Z}} \theta^{rp^j}$ on which σ acts by $(x_j)_{j \in \mathbf{Z}/g\mathbf{Z}} \mapsto (x_{j+a})_{j \in \mathbf{Z}/g\mathbf{Z}}$, where $a = [k : \mathbf{F}_p]$ and $g = af$.

Proof. Here we have abused notation to make $\chi \in \text{Hom}(T, l^\times)$ stand for an l -line on which T acts via χ . By the normal basis theorem [1, V.70], there exists a $\beta \in l$ such that the $\beta_j = \beta^{p^j}$ ($j \in \mathbf{Z}/g\mathbf{Z}$) constitute an \mathbf{F}_p -basis of l . When we fix such a β , we get a l -basis $\gamma_j = \beta_j \otimes 1$ of $l(r) \otimes_{\mathbf{F}_p[G]} l[G]$. The l -linear actions of σ and T on the γ_j are given by

$$\sigma.\gamma_j = (\beta^{p^j})^q \otimes 1 = \beta^{p^{j+a}} \otimes 1 = \gamma_{j+a}$$

and

$$t.\gamma_j = t.(\beta^{p^j} \otimes 1) = (t.\beta)^{p^j} \otimes 1 = \theta(t)^{rp^j} \gamma_j \quad (t \in T).$$

In other words, $l(r) \otimes_{\mathbf{F}_p[G]} l[G]$ is isomorphic to the direct sum of the characters θ^{rp^j} ($j \in \mathbf{Z}/g\mathbf{Z}$) which are permuted by σ according to $j \mapsto j + a$. \square

(12) The group $\text{Gal}(l|\mathbf{F}_p)$ acts on the set $\text{Hom}(T, l^\times)$ of characters of T : the generator $\varphi : x \mapsto x^p$ ($x \in l$) of $\text{Gal}(l|\mathbf{F}_p)$ sends a character $\chi \in \text{Hom}(T, l^\times)$ to χ^p .

(13) The $\mathbf{F}_p[G]$ -modules $l(r)$ and $l(s)$ are isomorphic if and only if the characters $\theta^r, \theta^s \in \text{Hom}(T, l^\times)$ are in the same φ -orbit.

Proof. The $\mathbf{F}_p[G]$ -modules $l(r)$ and $l(s)$ are isomorphic if and only if the $l[G]$ -modules $l(r) \otimes_{\mathbf{F}_p[G]} l[G]$ and $l(s) \otimes_{\mathbf{F}_p[G]} l[G]$ are isomorphic [1, V.70]. The result then follows from the explicit description (11) of the latter modules. \square

(14) Let n be a multiple of $\text{lcm}(p-1, e)$, and write $n = de$. The $\mathbf{F}_p[G]$ -module $M = \bigoplus_{i \in [1, n]} l(b^{(i)})$ is isomorphic to $k[G]^d$.

Proof. It is enough to show that the $l[G]$ -modules $M \otimes_{\mathbf{F}_p[G]} l[G]$ and $k[G]^d \otimes_{\mathbf{F}_p[G]} l[G]$ are isomorphic [1, V.70]. This follows from the description (11) of these modules, the criterion (13) for $l(r)$ and $l(s)$ to be $\mathbf{F}_p[G]$ -isomorphic, and the numerical lemma (5). \square

(15) The $k[G]$ -module (resp. $\mathbf{F}_p[G]$ -module) $l(r)$ is projective.

Proof. This follows from the fact that $l(r)$ is a direct summand (10) of the free module $k[G]$ (of rank 1 over $k[G]$ and rank a over $\mathbf{F}_p[G]$). \square

(16) (Iwasawa, [5, p. 449]) Let n be a multiple of $\text{lcm}(p-1, e)$, and

write $n = de$. Every $\mathbf{F}_p[G]$ -module M endowed with a filtration

$$\{0\} = M_{n+1} \subset M_n \subset \cdots \subset M_2 \subset M_1 = M$$

such that M_i/M_{i+1} is isomorphic to $l(b^{(i)})$ for $i \in [1, n]$ is isomorphic to $k[G]^d$.

Proof. As the $\mathbf{F}_p[G]$ -modules $l(r)$ are projective (15), the filtration on M splits in the sense that M is $\mathbf{F}_p[G]$ -isomorphic to $\bigoplus_{i \in [1, n]} l(b^{(i)})$. But this module is isomorphic to $k[G]^d$, as we have seen in (14). \square

3. The mixed-characteristic case

(17) Let K be a finite extension of \mathbf{Q}_p of ramification index e_K and residual degree f_K . Let L be a finite tamely ramified galoisian extension of K of ramification index e and residual degree f . Let L_0 be the maximal unramified extension of K in L and let $\Sigma = \text{Gal}(L_0|K)$, $T = \text{Gal}(L|K_0)$, and $G = \text{Gal}(L|K)$. Suppose that L is *split* over K in the sense that the short exact sequence $1 \rightarrow T \rightarrow G \rightarrow \Sigma$ has a section. Equivalently [5, 2.1], $L = L_0(\sqrt[e]{\pi_K})$ for some uniformiser π_K of K .

Let k (resp. l) be the residue field of K (resp. L). Identify Σ with $\text{Gal}(l|k)$, and let σ be the generator $x \mapsto x^q$ ($x \in l$, $q = p^{f_K}$) of Σ , so that $\sigma = \varphi^{f_K}$, in the notation of (12). The inertia group T comes equipped with a (faithful) character $\theta : T \rightarrow l^\times$ giving the action of T on the set of e -th roots of π_K , where π_K is any uniformier of K such that $L = L_0(\sqrt[e]{\pi_K})$. Thus, we are in the situation described in (7).

(18) Assume that the p -torsion subgroup ${}_pL^\times$ of L^\times has order p , so that the absolute ramification index e_L of L is divisible by $p - 1$; write $e_L = c(p - 1)$. Note that every finite tamely ramified extension of K is contained in a finite galoisian tamely ramified split extension of K containing a primitive p -th root of 1.

(19) For $r > 0$, denote by \bar{U}_L^r the G -submodule the image of U_L^r in $\bar{L}^\times = L^\times/L^{\times p}$, where $U_L^r = 1 + \mathfrak{p}_L^r$ and \mathfrak{p}_L is the unique maximal ideal of the ring of integers \mathfrak{o}_L of L . Note that \bar{U}_L^1 is equal to the image $\overline{\mathfrak{o}_K^\times}$ of the group \mathfrak{o}_L^\times of units of \mathfrak{o}_L . It is known that $\bar{U}_L^r = \{1\}$ for $r > cp$, that \bar{U}_L^{cp} is $\mathbf{F}_p[G]$ -isomorphic to ${}_pL^\times$ (but the submodule $\bar{U}_L^{cp} \subset \bar{L}^\times$ is not to be confused with the submodule ${}_pL^\times \subset L^\times$ nor with its image $\overline{{}_pL^\times} \subset \bar{L}^\times$), that $\bar{U}_L^{ip} = \bar{U}_L^{ip+1}$ for $i \in [1, c[$ and that $\bar{U}_L^r/\bar{U}_L^{r+1}$ is isomorphic to $l(r)$ for $r \in [1, cp[$, $r \not\equiv 0 \pmod{p}$, where $l(r)$ is the $k[G]$ -module l with σ acting by $x \mapsto x^q$ and T acting by the character θ^r , as in (9). See for example [3], where we had $L = K(\sqrt[p-1]{K^\times})$ but the same proofs work without change.

(20) Take $n = e_L$, which is a multiple of $\text{lcm}(p-1, e)$ (18), as required in (16), and note that $cp = b^{(n)} + 1$. For every $i \in [1, n]$, put $M_i = \bar{U}_L^{b^{(i)}} / \bar{U}_L^{cp}$ and put $M_{n+1} = \{1\}$. This filtration on the $\mathbf{F}_p[G]$ -module $M = M_1$ has the property that M_i/M_{i+1} is isomorphic to $l(b^{(i)})$ for every $i \in [1, n]$, as we have recalled (19). It follows from Iwasawa's lemma (16) that M is isomorphic to $k[G]^{e_K}$, and hence \bar{U}_L^1 is isomorphic to ${}_pL^\times \oplus k[G]^{e_K}$. In summary, we get the following result of Iwasawa [5, p. 461].

(21) *Let K be a finite extension of \mathbf{Q}_p of ramification index e_K and residue field k , and let L be a finite galoisian tamely ramified split extension of K of group $G = \text{Gal}(L|K)$ such that ${}_pL^\times$ has order p . The $\mathbf{F}_p[G]$ -module \bar{U}_L^1 is isomorphic to ${}_pL^\times \oplus k[G]^{e_K}$, which is isomorphic to ${}_pL^\times \oplus \mathbf{F}_p[G]^{[K:\mathbf{Q}_p]}$. \square*

(22) Let $\bar{\mathbf{F}}_p$ be the maximal galoisian extension of \mathbf{F}_p . As a corollary, we deduce that the $\bar{\mathbf{F}}_p[G]$ -module $M \otimes_{\mathbf{F}_p[G]} \bar{\mathbf{F}}_p[G]$ is isomorphic to $\bar{\mathbf{F}}_p[G]^{[K:\mathbf{Q}_p]}$, thereby recovering [4, Corollary 4.7]. Our method also shows that if L is a finite galoisian tamely ramified split extension of K such that ${}_pL^\times$ is trivial but e_L is divisible by $p-1$, then the $\mathbf{F}_p[G]$ -module $\bar{U}_L^1 = \overline{\mathfrak{o}_L^\times}$ is isomorphic to $k[G]^{e_K}$ and to $\mathbf{F}_p[G]^{[K:\mathbf{Q}_p]}$, for the only difference in this case is that \bar{U}_L^{cp} is trivial.

(23) As a curiosity, the reader may wish to determine the structure of the $\mathbf{F}_p[G]$ -modules $\prod_{i>0} U_L^{b^{(i)}} / U_L^{b^{(i)}+1}$ and $\bigoplus_{i>0} \mathfrak{p}_L^{-b^{(i)}} / \mathfrak{p}_L^{-b^{(i)}+1}$, where $b^{(i)}$ is the sequence of positive integers $\not\equiv 0 \pmod{p}$, as throughout.

4. The equi-characteristic case

(24) Let K be a local field of characteristic p with finite residue field k of cardinality q , and let L be a finite galoisian tamely ramified split extension of K of ramification index e ($\not\equiv 0 \pmod{p}$) and residual degree f (so that $q^f \equiv 1 \pmod{e}$). Every finite tamely ramified extension of K is contained in such an L . Concretely, the residue field l of L is the finite extension of k of degree f and there is a uniformiser π_K of K such that $K = k((\pi_K))$ and $L = l((\sqrt[e]{\pi_K}))$. The groups $\Sigma = \text{Gal}(l|k)$, $G = \text{Gal}(L|K)$, $T = \text{Gal}(L|l((\pi_K)))$ and the character $\theta : T \rightarrow l^\times$ giving the action of T on the set of e -th roots of π_K have the properties required in (7).

(25) Let us determine the structure of the $\mathbf{F}_p[G]$ -module $L^+/\wp(L^+)$, where $\wp(x) = x^p - x$ ($x \in L$). It will turn out that $L^+/\wp(L^+)$ is isomorphic to $\mathbf{F}_p \oplus k[G]^{(N)}$, just as in the case $e = p-1$, $f = p-1$ treated in [3]. The proof combines ideas from [3] with Iwasawa's lemma (16), and is analogous to the proof of (21).

(26) Let \mathfrak{p}_L be the unique maximal ideal of the ring of integers $\mathfrak{o}_L = l[[\sqrt[p]{\pi_K}]]$ of L . For every $r \in \mathbf{Z}$, denote by $\overline{\mathfrak{p}_L^r}$ the G -submodule the image of \mathfrak{p}_L^r in $\overline{L^+} = L^+/\wp(L^+)$. It is known that $\overline{\mathfrak{p}_L^r} = \{0\}$ for $r > 0$, that $\overline{\mathfrak{o}_L^+} = \overline{\mathfrak{p}_L^0}$ is canonically isomorphic to \mathbf{F}_p , that $\overline{\mathfrak{p}_L^{ip+1}} = \overline{\mathfrak{p}_L^{ip}}$ for all $i < 0$, and that $\overline{\mathfrak{p}_L^r}/\overline{\mathfrak{p}_L^{r+1}}$ is isomorphic to $l(r)$ for every $r < 0$, $r \not\equiv 0 \pmod{p}$, in the notation of (9). See for example [2] for the general case and [3] for the special case $L = K(\sqrt[p-1]{K^\times})$.

(27) Let n be a multiple of $\text{lcm}(p-1, e)$ (16), write $n = c.(p-1)$, $n = d.e$ and note that $cp = b^{(n)} + 1$. For $i \in [1, n]$, put $\lambda(i) = b^{(i)} - cp$ and define $M_i = \overline{\mathfrak{p}_L^{\lambda(i)}}/\overline{\mathfrak{p}_L^0}$; also put $M_{n+1} = \{0\}$. We thus get a filtration on the $\mathbf{F}_p[G]$ -module $M = M_1$ such that M_i/M_{i+1} is isomorphic to $l(b^{(i)} - c)$ for every $i \in [1, n]$, since $\lambda(i) \equiv b^{(i)} - c \pmod{e}$. Replacing n by a suitable multiple of n , we may assume that $c \equiv 0 \pmod{e}$ and therefore that M_i/M_{i+1} is isomorphic to $l(b^{(i)})$. Since M is isomorphic to $k[G]^d$ (16), $\overline{\mathfrak{p}_L^{-b^{(n)}}}$ is $\mathbf{F}_p[G]$ -isomorphic to $\mathbf{F}_p \oplus k[G]^d$ (26).

(28) Replacing n by mn ($m > 0$), we conclude that $\overline{\mathfrak{p}_L^{-b^{(mn)}}}$ is $\mathbf{F}_p[G]$ -isomorphic to $\mathbf{F}_p \oplus k[G]^{md}$. As L^+ is the direct limit of the $\overline{\mathfrak{p}_L^{-b^{(mn)}}}$ when $m \rightarrow +\infty$, we conclude that $L^+/\wp(L^+)$ is isomorphic to $\mathbf{F}_p \oplus k[G]^{(\mathbf{N})}$, just as in the case $L = K(\sqrt[p-1]{K^\times})$ treated earlier [3]. Let us summarise.

(29) *Let K be local field of characteristic p with finite residue field k , let L be a finite galoisian tamely ramified split extension of K , and let $G = \text{Gal}(L|K)$. The $\mathbf{F}_p[G]$ -module $\overline{L^+} = L^+/\wp(L^+)$ is isomorphic to $\mathbf{F}_p \oplus k[G]^{(\mathbf{N})}$ and to $\mathbf{F}_p \oplus \mathbf{F}_p[G]^{(\mathbf{N})}$.* \square

(30) While we are at it, we might as well determine the structure of the $\mathbf{F}_p[G]$ -module \bar{U}_L^1 , where \bar{U}_L^r ($r > 0$) is the image of $U_L^r = 1 + \mathfrak{p}_L^r$ in $L^\times/L^{\times p}$. It is easy to see that $\bar{U}_L^{ip} = \bar{U}_L^{ip+1}$ for every $i > 0$ and that $\bar{U}_L^r/\bar{U}_L^{r+1}$ is $\mathbf{F}_p[G]$ -isomorphic to $l(r)$ for every $r > 0$, $r \not\equiv 0 \pmod{p}$.

(31) Let n be a multiple of $\text{lcm}(p-1, e)$ (14), with $n = c.(p-1)$, $n = d.e$. For $i \in [1, n]$, put $M_i = \bar{U}_L^{b^{(i)}}/\bar{U}_L^{cp}$, and put $M_{n+1} = \{1\}$. This filtration on the module $M = M_1$ has the properties required for applying Iwasawa's lemma (16), therefore $\bar{U}_L^1/\bar{U}_L^{cp}$ is isomorphic to $k[G]^d$. Replacing n by a multiple mn , we see that $\bar{U}_L^1/\bar{U}_L^{mcp}$ is isomorphic to $k[G]^{md}$. Taking the projective limit as $m \rightarrow +\infty$, we get the structure of \bar{U}_L^1 :

(32) *The image \bar{U}_L^1 of $U_L^1 = 1 + \mathfrak{p}_L$ in $L^\times/L^{\times p}$ is $\mathbf{F}_p[G]$ -isomorphic to $k[G]^{(\mathbf{N})}$ and to $\mathbf{F}_p[G]^{(\mathbf{N})}$.* \square

5. Passing to the tame limit

(33) Let K be a local field with finite residue field k of characteristic p and cardinality q , V the maximal tamely ramified extension of K , and B the maximal abelian extension of V of exponent p , so that $B = V(\sqrt[p]{V^\times})$ if K has characteristic 0 and $B = V(\wp^{-1}(V))$ if K has characteristic p . The pro- p -group $\text{Gal}(B|V)$ is an $\mathbf{F}_p[[\Gamma]]$ -module, where $\Gamma = \text{Gal}(V|K)$, and we would like to determine its structure. This is achieved by studying the dual $\mathbf{F}_p[[\Gamma]]$ -module, namely $V^\times/V^{\times p}$ in characteristic 0 and $V^+/\wp(V^+)$ in characteristic p .

(34) If K has characteristic 0, there is an interesting intermediate extension B' which may be called the maximal *peu ramifiée* extension of V (in B); it is obtained by adjoining $\sqrt[p]{u}$ to V for every $u \in \mathfrak{o}_V^\times$, where \mathfrak{o}_V is the ring of integers of V . As $B = B'(\sqrt[p]{\pi})$ for every uniformiser π of K , the group $\text{Gal}(B|B')$ is cyclic of order p , the short exact sequence

$$\{1\} \rightarrow \text{Gal}(B|B') \rightarrow \text{Gal}(B|K) \rightarrow \text{Gal}(B'|K) \rightarrow \{1\}$$

of profinite groups splits, and the resulting conjugation action of $\text{Gal}(B'|K)$ on $\text{Gal}(B|B')$ is given by the cyclotomic character $\omega : \text{Gal}(B'|K) \rightarrow \mathbf{F}_p^\times$. It follows from [5, Lemma 4] that the short exact sequence

$$\{1\} \rightarrow \text{Gal}(B'|V) \rightarrow \text{Gal}(B'|K) \rightarrow \Gamma \rightarrow \{1\}$$

of profinite groups also splits. As the $\mathbf{F}_p[[\Gamma]]$ -module $\text{Gal}(B'|V)$ is isomorphic to $\text{Hom}(\mathfrak{o}_V^\times/\mathfrak{o}_V^{\times p}, {}_pV^\times)$, it is sufficient to determine the structure of the $\mathbf{F}_p[[\Gamma]]$ -module $\mathfrak{o}_V^\times/\mathfrak{o}_V^{\times p}$, which we do.

(35) Similarly, if K has characteristic p , then the short exact sequence

$$\{1\} \rightarrow \text{Gal}(B|V) \rightarrow \text{Gal}(B|K) \rightarrow \Gamma \rightarrow \{1\}$$

of profinite groups splits. As the $\mathbf{F}_p[[\Gamma]]$ -module $\text{Gal}(B|V)$ is isomorphic to $\text{Hom}(V^+/\wp(V^+), \mathbf{F}_p)$, it is sufficient to determine the structure of $V^+/\wp(V^+)$, which is done below.

(36) Let V_0 be the maximal unramified extensions of K (in V). For every $n > 0$, put $e_n = q^n - 1$, $K_n = K(\sqrt[p]{1})$ and $L_n = K_n(\sqrt[p]{K_n^\times})$. Note that L_n is the maximal abelian extension of K_n of exponent dividing e_n , so it is galoisian over K ; put $G_n = \text{Gal}(L_n|K)$. The ramification index (resp. the residual degree) of L_n over K is e_n (resp. ne_n). We have

$$V_0 = \varinjlim K_n, \quad V = \varinjlim L_n, \quad \Gamma = \varprojlim G_n.$$

Note that if K has characteristic 0, then the p -torsion subgroup ${}_pL_n^\times$ of L_n^\times has order p (because L_1 contains $\sqrt[p-1]{-p}$).

(37) Assume that K has characteristic 0. For every finite extension L of K , denote by e_L ramification index of $L|\mathbf{Q}_p$. As $e_{L_n} \equiv 0 \pmod{e_n}$, we have $e_{L_n} \equiv 0 \pmod{p-1}$, for every $n > 0$; write $e_{L_n} = c_n \cdot (p-1)$. We have seen (20) that the $\mathbf{F}_p[G_n]$ -module $M_n = \bar{U}_{L_n}^1 / \bar{U}_{L_n}^{c_n \cdot p}$ is isomorphic to $k[G_n]^{e_K}$. Also, for every multiple m of n , the map $M_n \rightarrow M_m$ induced by the inclusion $L_n \subset L_m$ is *injective*. As $\mathfrak{o}_V^\times / \mathfrak{o}_V^{\times p} = \varinjlim M_n$, we get from (21) by passage to the limit :

(38) Let K be a finite extension of \mathbf{Q}_p of residue field k and ramification index e_K , let V be the maximal tamely ramified extension of K , and let $\Gamma = \text{Gal}(V|K)$. The $\mathbf{F}_p[[\Gamma]]$ -module $\mathfrak{o}_V^\times / \mathfrak{o}_V^{\times p}$ is isomorphic to $k[[\Gamma]]^{e_K}$, and the $\mathbf{F}_p[[\Gamma]]$ -module $V^\times / V^{\times p}$ is isomorphic to $k[[\Gamma]]^{e_K} \oplus \mathbf{F}_p$. \square

(39) As for the dual $\mathbf{F}_p[[\Gamma]]$ -modules $\text{Gal}(B'|V) = \text{Hom}(\mathfrak{o}_V^\times / \mathfrak{o}_V^{\times p}, {}_pV^\times)$ and $\text{Gal}(B|V) = \text{Hom}(V^\times / V^{\times p}, {}_pV^\times)$, they are respectively isomorphic to $k[[\Gamma]]^{e_K}$ and to ${}_pV^\times \oplus k[[\Gamma]]^{e_K}$. Note that $k[[\Gamma]]^{e_K}$ is free of rank $[K : \mathbf{Q}_p]$ over $\mathbf{F}_p[[\Gamma]]$.

(40) Now suppose that K has characteristic p . By an entirely similar argument, working with the modules $M_n = \bar{L}_n^+ / \bar{\mathfrak{o}}_{L_n}^+$ (resp. $\bar{\mathfrak{o}}_{L_n}^\times$, resp. \bar{L}_n^\times), one gets from (29) and (32) by passage to the limit :

(41) For $K = k((t))$, the $\mathbf{F}_p[[\Gamma]]$ -module $\bar{V}^+ = V^+ / \wp(V^+)$ is isomorphic to $\mathbf{F}_p[[\Gamma]]^{(\mathbf{N})}$, and the $\mathbf{F}_p[[\Gamma]]$ -modules $\bar{\mathfrak{o}}_V^\times = \mathfrak{o}_V^\times / \mathfrak{o}_V^{\times p}$ and $\bar{V}^\times = V^\times / V^{\times p}$ are isomorphic to $\mathbf{F}_p[[\Gamma]]^{\mathbf{N}}$. \square

(42) As a result, the $\mathbf{F}_p[[\Gamma]]$ -module $\text{Gal}(B|V) = \text{Hom}(V^+ / \wp(V^+), \mathbf{F}_p)$ is isomorphic to $\mathbf{F}_p[[\Gamma]]^{\mathbf{N}}$.

6. Coronidis loco

(43) Let K be a p -field and let \tilde{K} be a maximal galoisian extension of K . It is clear that if K has characteristic p , then the profinite group $\text{Gal}(\tilde{K}|K)$ cannot be finitely generated, because K has infinitely many cyclic extensions of degree p : the dimension of the \mathbf{F}_p -space $K^+ / \wp(K^+)$ is infinite. It is common knowledge that if K is a finite extension of \mathbf{Q}_p , then $\text{Gal}(\tilde{K}|K)$ can be generated by $[K : \mathbf{Q}_p] + 3$ elements, cf. [6, p. 65]. As a small gift for the reader who has made it so far, we indicate how the foregoing can be used to give a nice little proof ; it relies on the following observation about profinite groups.

(44) We say that a subset S of a profinite group G *generates* G if G is the only *closed* subgroup of G containing S . A *finite* subset Π of a pro- p -group P generates P if and only if its image $\bar{\Pi}$ in the maximal commutative quotient \bar{P} of P of exponent dividing p generates \bar{P} (Burnside's "basis"

theorem) ; see [7, 4.10].

(45) Consider a short exact sequence $\{1\} \rightarrow P \rightarrow G \rightarrow \Delta \rightarrow \{1\}$ of profinite groups such that P is a pro- p -group (and a closed subgroup of G), so that \bar{P} is an $\mathbf{F}_p[[\Delta]]$ -module. Presumably, *if $\Pi \subset P$ is a finite subset whose image in \bar{P} generates the $\mathbf{F}_p[[\Delta]]$ -module \bar{P} , and if $D \subset G$ is a finite subset whose image in Δ generates Δ , then their union $\Pi \cup D$ generates G* . This should follow from an argument similar to the one in [6, Lemma 3.3]. In our application below, the extension G of Δ by P splits.

(46) If this presumption is true, then (39) provides a simple proof of the fact that the profinite group $G = \text{Gal}(\tilde{K}|K)$ is generated by $[K : \mathbf{Q}_p] + 3$ elements. Indeed, take $P = \text{Gal}(\tilde{K}|V)$, so that $G/P = \Gamma$ and $\bar{P} = \text{Gal}(B|V)$. We know from Iwasawa [5, Theorem 2] that Γ is generated by *two* elements (and moreover the extension G of Γ by P splits). We have seen (39) that the $\mathbf{F}_p[[\Gamma]]$ -module $\text{Gal}(B|V)$ is generated by $[K : \mathbf{Q}_p] + 1$ elements. Hence, if (45) holds, then G is generated by $[K : \mathbf{Q}_p] + 3$ elements.

BIBLIOGRAPHY

- [1] BOURBAKI (N). — *Algèbre, Chapitres 4 à 7*, Masson, Paris, 1981, 422 pp.
- [2] DALAWAT (C). — *Further remarks on local discriminants*, J. Ramanujan Math. Soc. bf 25 (2010) 4, 393–417. Cf. arXiv:0909.2541.
- [3] DALAWAT (C). — *Serre’s “formule de masse” in prime degree*, Monatshefte Math. **166** (2012) 1, 73–92. Cf. arXiv:1004.2016.
- [4] DEL CORSO (I), DVORNICICH (R) & MONGE (M). — *On wild extensions of a p -adic field*, J. Number Theory **174** (2017), 322–342. Cf. aXiv:1601.05939.
- [5] IWASAWA (K). — *On Galois groups of local fields*. Trans. Amer. Math. Soc. **80** (1955), 448–469.
- [6] JANNSSEN (U). — *Über Galoisgruppen lokaler Körper*. Invent. Math. **70** (1982/83) 1, 53–69.
- [7] KOCH (H). — *Galois theory of p -extensions*. Springer-Verlag, Berlin, 2002, 190 pp.